BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	101 38 014.3
Anmeldetag:	2. August 2001
Anmelder/Inhaber:	Leopold Kostal GmbH & Co KG, Lüdenscheid/DE
Bezeichnung:	Schlüssellose Zugangsberechtigungskontroll-einrichtung
IPC:	G 07 C, E 05 B und H 04 L

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 26. Juni 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Hoiß

A 9161
03/00
EDV-L

Zusammenfassung

Die vorliegende Erfindung betrifft eine schlüssellose Zugangsberechtigungskontrolleinrichtung mit zumindest zwei, jeweils einem bestimmten Objekt zugeordneten, Sende-/Empfangseinrichtungen umfassenden Objektmodulen und mit einem oder mehreren, jeweils zumindest einen Mikroprozessor aufweisenden Identifikationsgebern, wobei jeweils über eine bidirektionale Datenkommunikationsstrecke Daten zwischen dem/den Identifikationsgeber(n) und den Objektmodulen übertragbar sind, welche Daten mittels eines einen Verschlüsselungsalgorithmus sowie dem jeweiligen Objektmodul zugeordnete Verschlüsselungsparameter verwendenden, symmetrischen Verschlüsselungsverfahrens codiert sind. Gegenüber dem bekannten Stand der Technik weist die erfindungsgemäße Einrichtung eine deutlich höhere Flexibilität für die Anpassung an sich ändernde Randbedingungen auf, da bei dieser von vornherein der Einsatz zumindest zweier unterschiedlicher Verschlüsselungsalgorithmen vorgesehen ist.

Lüdenscheid, den 31.07.2001
R 1420
ANR: 1 535 978

Anmelderin: Firma
Leopold Kostal GmbH & Co. KG
Wiesenstr. 47
58507 Lüdenscheid

Schlüssellose Zugangsberechtigungskontrolleinrichtung

Beschreibung

Die vorliegende Erfindung betrifft eine schlüssellose Zugangsberechtigungskontrolleinrichtung mit zumindest zwei, jeweils einem bestimmten Objekt zugeordneten, Sende-/Empfangseinrichtungen umfassenden Objektmodulen und mit einem oder mehreren, jeweils zumindest einen Mikroprozessor aufweisenden Identifikationsgebern, wobei jeweils über eine bidirektionale Datenkommunikationsstrecke Daten zwischen dem/den Identifikationsgeber(n) und den Objektmodulen übertragbar sind, welche Daten mittels eines einen Verschlüsselungsalgorithmus sowie dem jeweiligen Objektmodul zugeordnete Verschlüsselungsparameter verwendenden, symmetrischen Verschlüsselungsverfahrens codiert sind.

Ferner betrifft die Erfindung einen Identifikationsgeber sowie ein Objektmodul für eine solche schlüssellose Zugangsberechtigungskontrolleinrichtung.

Schlüssellose Zugangsberechtigungskontrolleinrichtungen werden dort eingesetzt, wo eine Zugangskontrolle mittels eines mechanischen Schlüssels

nicht gewünscht ist. Derartige Zugangsberechtigungskontrolleinrichtungen werden beispielsweise bei Kraftfahrzeugen und im Hausbereich eingesetzt. Das bestimmungsgemäße Öffnen des jeweiligen Objekts, beispielsweise des Kraftfahrzeugs oder des Hauses, erfolgt drahtlos durch Übertragen eines entsprechenden Befehls zusammen mit einem codierten Datensatz (kurz: Code) von einem von einem Benutzer mitgeführten Identifikationsgeber an eine jeweils dem gewünschten Objekt zugeordnete Sende-/Empfangseinrichtung. Wird von der objektgebundenen Sende-/Empfangseinrichtung der dem Objekt zugehörige Code empfangen, gilt die den Identifikationsgeber mitführende Person als zugangsberechtigt, so daß anschließend zum Ermöglichen eines Zugangs bestimmte Aktoren angesteuert werden, um darüber beispielsweise das Kraftfahrzeug zu entriegeln. Damit bei einer Verwendung mehrerer schlüsselloser Zugangsberechtigungskontrolleinrichtungen nicht mehrere Identifikationsgeber mitgeführt werden müssen, sind Identifikationsgeber und entsprechende Zugangsberechtigungskontrolleinrichtungen entwickelt worden, bei denen ein einziger Identifikationsgeber für eine Zugangsberechtigungskontrollabfrage bei mehreren Objekten, beispielsweise dem Kraftfahrzeug, dem Haus und ggf. der Arbeitsstelle benutzt werden kann.

Die vorbekannten Einrichtungen, bei denen mit einem Identifikationsgeber eine Zugangsberechtigungskontrolle bei mehreren Objekten durchgeführt werden kann, arbeiten nach dem Prinzip, daß sämtliche objektbezogenen Sende-/Empfangseinrichtungen mit demselben Verschlüsselungsalgorithmus arbeiten. Derartige Einrichtungen sind etwa aus der DE 195 33 309 A1 oder der DE 196 07 017 C2 bekannt.

Beim Gegenstand der DE 195 33 309 A1 ist der übertragene Code zusammengesetzt aus einem Festcode und einem Wechselcode, die beide gemeinsam zum Öffnen eines Kraftfahrzeugs gesendet werden. Um im

Rahmen einer solchen Zugangsberechtigungskontrolleinrichtung auch Personen mit Identifikationsgebern ausstatten zu können, die lediglich das Haus, nicht jedoch das Kraftfahrzeug öffnen dürfen, sind im Rahmen dieser Zugangsberechtigungskontrolleinrichtung ein oder mehrere weitere Identifikationsgeber vorgesehen, die nur einen Code – den Wechselcode – senden.

Beim Gegenstand der DE 196 07 017 C2 werden jeweils über eine bidirektionale Datenkommunikationsstrecke Daten zwischen dem Identifikationsgeber und den den Objekten zugeordneten Sende-/Empfangseinrichtungen übertragen, wobei die Daten mittels eines symmetrischen Verschlüsselungsverfahrens codiert sind. Die übertragenen Daten werden dabei mittels eines zur Realisierung des symmetrischen Verschlüsselungsverfahrens eingesetzten Verschlüsselungsalgorithmus' unter Verwendung bestimmter Verschlüsselungsparameter codiert, wobei diese Verschlüsselungsparameter als sogenanntes Verschlüsselungsgeheimnis dem jeweils angesprochenen Objekt zugeordnet sind. Bei dieser Einrichtung ist ein Abgleich der Verschlüsselungsparameter zwischen Identifikationsgeber und dem jeweiligen Objekt in einem sogenannten Lernmodus vorgesehen.

Gemeinsames Charakteristikum dieser vorbekannten Einrichtungen bzw. Identifikationsgeber ist, daß für die Zugangsberechtigung bei unterschiedlichen Objekten die Verwendung ein und desselben Verschlüsselungsalgorithmus' vorgesehen ist. Die hieraus resultierende geringe Flexibilität ist insbesondere bei solchen Objekten von Nachteil, die eine unterschiedliche Lebenserwartung aufweisen, wie beispielweise ein Kraftfahrzeug und ein Haus. Beim Wechsel eines der beiden Objekte ist nicht unbedingt sichergestellt, daß das neu hinzugekommene Objekt mit dem gleichen Verschlüsselungsalgorithmus arbeitet, so daß wahrscheinlich auch ein Wechsel des dem verbliebenen Objekt zugehörigen Objektmoduls

erforderlich ist. Insbesondere bei einer noch größeren Anzahl von Objekten ist der Konflikt beim Wechsel eines der Objekte oder beim Hinzukommen eines weiteren Objekts oder Identifikationsgebers nahezu unvermeidbar.

Demgegenüber weist die erfindungsgemäße Einrichtung eine deutlich höhere Flexibilität für die Anpassung an sich ändernde Randbedingungen auf, da bei dieser von vornherein der Einsatz zumindest zweier unterschiedlicher Verschlüsselungsalgorithmen vorgesehen ist, und zwar in einer ersten Ausführungsform in dem Identifikationsgeber und in einer zweiten Ausführungsform in zumindest einem der Objektmodule (vorzugsweise in dem mit der längsten Lebensdauer, wie z.B. einem Haus). Dadurch ist es beispielsweise bei der ersten Ausführungsform möglich, beim Wechsel eines Objektes in dem Identifikationsgeber für das neue Objektmodul einen anderen Verschlüsselungsalgorithmus auszuwählen oder erforderlichenfalls durch eine Umprogrammierung des Identifikationsgebers einen alten Verschlüsselungsalgorithmus durch einen neuen zu ersetzen, ohne dabei die anderen, in den verbliebenen Objektmodulen implementierten Verschlüsselungsalgorithmen zu beeinflussen. Die zweite Ausführungsform ist insbesondere in dem Fall vorteilhaft, daß z.B. das bisherige Fahrzeug durch ein neues ersetzt wird, und damit gleichzeitig ein neuer Identifikationsgeber den dem alten Fahrzeug zugehörigen ersetzt, wobei der neue Identifikationsgeber mit einem anderen Verschlüsselungalgorithmus arbeitet als der alte. In diesem Falle wird der von dem neuen Identifikationsgeber verwendete Verschlüsselungsalgorithmus in dem anderen Objektmodul, z.B. dem des Hauses – soweit bereits in dem Speicherelement desselben vorhanden – für diesen Identifikationsgeber aktiviert, oder andernfalls durch Umprogrammierung an Stelle des alten, nicht mehr benötigten Verschlüsselungsalgorithmus' abgelegt, ohne dabei andere, weitere

Identifikationsgeber betreffende Verschlüsselungsalgorithmen zu beeinflussen.

Nachfolgend ist die Erfindung anhand eines Ausführungsbeispiels unter Bezugnahme auf die beigefügten Figuren beschrieben.

Dabei zeigen

Fig. 1: Eine schematisierte Darstellung einer erfindungsgemäßen schlüssellosen Zugangsberechtigungskontrolleinrichtung nach einer ersten Ausführungsform.

Fig. 2: Eine Alternative zu dem in Fig. 1 dargestellten Identifikationsgeber

Ein Identifikationsgeber 10 dient im Rahmen einer schlüssellosen Zugangsberechtigungskontrolleinrichtung dazu, einem Benutzer eine Zugangsberechtigung zu mehreren Objekten zu beschaffen. Der in Fig. 1 dargestellte Identifikationsgeber 10 enthält die notwendigen elektrischen Sende-/Empfangsmittel 13, um eine Kommunikation mit Sende-/ Empfangseinrichtungen 4, 5 der den jeweiligen Objekten zugeordneten Objektmodule 1, 2 durchführen und dabei zur Feststellung der Zugangsberechtigung codierte Daten über bidirektionale Datenkommunikationsstrecken 14, 15 austauschen zu können. Die Codierung der Daten erfolgt dabei sowohl in dem Identifikationsgeber 10 als auch in den Objektmodulen 1, 2 durch Mikroprozessoren 11, 6, 7 unter Verwendung eines symmetrischen Verschlüsselungsverfahrens, wobei der Identifikationsgeber 10 und das jeweils angesprochene Objektmodul 1, 2 zur Verschlüsselung der Daten die gleichen Verschlüsselungsparameter P1, P2 verwenden. Diese Verschlüsselungsparameter stellen das jeweils zwischen dem Identifikationgeber 10 und einem der Objektmodule 1, 2 bestehende

Verschlüsselungsgeheimnis dar. In dem Identifikationsgeber 10 ist in einem Speicherelement 12 für jedes Objektmodul 1, 2 ein separater Satz von Verschlüsselungsparametern P1, P2 abgelegt, welche sich voneinander unterscheiden. Jeder dieser Sätze von Verschlüsselungsparametern P1, P2 kann dabei im Zuge eines Datenaustausches zwischen dem Identifikationsgeber 10 und dem den jeweiligen Parametersatz verwendenden Objektmodul 1, 2 in Abstimmung auf beiden Seiten in bekannter Weise verändert werden, um ein Ausspionieren des Verschlüsselungsgeheimnisses zu verhindern. Neben den Verschlüsselungsparametern P1, P2 sind in dem Speicherelement 12 des Identifikationsgebers 10 auch verschiedene, zur Durchführung eines symmetrischen Verschlüsselungverfahrens geeignete und gebräuchliche Verschlüsselungsalgorithmen A1, A2, ... abgelegt, wobei jedem Objektmodul 1, 2 jeweils ein Verschlüsselungsalgorithmus fest zugeordnet ist, und zwar derjenige, welcher auch von dem jeweiligen Objektmodul 1, 2 selbst verwendet wird. Die feste Zuordnung des von dem Identifikationsgeber in Bezug auf das jeweilige Objektmodul zu verwendenden Verschlüsselungsalgorithmus geschieht sozusagen beim „Kennenlernen" der beiden Einrichtungen durch einen einmaligen Initialisierungsvorgang. Im Gegensatz zu den Verschlüsselungsparametern P1, P2 , die in ihrer jeweils gerade gültigen Form charakteristisch für das jeweilige Objektmodul 1, 2 sind, unterscheiden sich die von den Objektmodulen 1, 2 verwendeten Verschlüsselungsalgorithmen nicht notwendigerweise voneinander. Es kann also z.B. durchaus vorkommen, daß mehrere Objektmodule 1, 2, 3, ... ein und denselben Algorithmus – z.B. etwa A1 – verwenden, während nur ein einziges Objektmodul N einen anderen Algorithmus A2 verwendet, oder ähnliche Kombinationen. Entscheidend ist, daß in dem Identifikationsgeber 10 eine Mehrzahl von gebräuchlichen Algorithmen A1, A2, ... abgelegt ist, die im Bedarfsfalle, z.B. bei Hinzukommen eines neuen Objektmoduls von dem Mikroprozessor 11 aufgerufen werden können. Aus dem Vorrat an

Verschlüsselungsalgorithmen A1, A2, ..., die sich im Speicherelement 12 des Identifikationsgebers 10 befinden, können über eine Programmierungsschnittstelle auch einzelne, nicht benötigte Algorithmen durch neuere ersetzt werden, ohne die für andere Objektmodule nach wie vor benötigten Algorithmen zu beeinflussen.

Der in Fig. 2 dargestellte alternative Identifikationsgeber 10 unterscheidet sich insofern von dem in Fig. 1, als hier statt nur eines Mikroprozessors 11 der Einsatz von zwei unabhängigen Mikroprozessoren 11 und 11' vorgesehen ist, wobei die den Mikroprozessoren zugeordneten Speicherelemente 12 und 12' in diesen jeweils direkt integriert sind. Eine derartige Integration eines Speicherelements 12 in dem Mikroprozessor 11 ist selbstverständlich auch bei dem in Fig. 1 dargestellten Identifikationsgeber 10 möglich. Die in Fig. 2 gezeigte Ausführung bietet diesem gegenüber jedoch den den Vorteil, daß der zweite Mikroprozessor 11' mit den in seinem Speicher 12' abgelegten zusätzlichen Algorithmen im Bedarfsfalle auch komplett hardwaremäßig austauschbar ist, so daß eine Umprogrammierung auch dann nicht erforderlich ist, wenn ein bis dahin nicht zur Verwendung vorgesehener Algorithmus verwendet werden soll. Der erste Mikroprozessor 11 mit seinem Speicher 12 verbleibt dagegen im Identifikationsgeber 10, so daß dessen Funktion im Zusammenhang mit dem oder den weiterhin verwendeten Objektmodul(en) durch den Austausch nicht beeinflußt wird.

Während die bisher beschriebene erste Ausführungsform der erfindungsgemäßen, schlüssellosen Zugangsberechtigungskontrolleinrichtung sozusagen von einem universellen Identifikationsgeber ausgeht, welcher mit mehreren, verschiedene Verschlüsselungsalgorithmen verwendenden Objektmodulen kooperieren kann, ist in einer zweiten Ausführungsform vorgesehen, daß zumindest ein universelles Objektmodul vorhanden ist,

welches seinerseits mit mehreren, verschiedene Verschlüsselungsalgorithmen verwendenden Identifikationsgebern kooperieren kann. Selbstverständlich ist in einer Maximalkonfiguration auch die gleichzeitige Verwendung sowohl universeller Identifikationsgeber als auch universeller Objektmodule möglich.

Patentansprüche

1. Schlüssellose Zugangsberechtigungskontrolleinrichtung mit zumindest zwei, jeweils einem bestimmten Objekt zugeordneten, Sende-/Empfangseinrichtungen (4, 5) umfassenden Objektmodulen (1, 2) und mit einem oder mehreren, jeweils zumindest einen Mikroprozessor (11, 11') aufweisenden Identifikationsgebern (10), wobei jeweils über eine bidirektionale Datenkommunikationsstrecke (14, 15) Daten zwischen dem Identifikationsgeber (10) und den Objektmodulen (1, 2) übertragbar sind, welche Daten mittels eines einen Verschlüsselungsalgorithmus sowie dem jeweiligen Objektmodul (1, 2) zugeordnete Verschlüsselungsparameter (P1, P2) verwendenden, symmetrischen Verschlüsselungsverfahrens codiert sind, **dadurch gekennzeichnet,** daß in (einem) in dem Identifikationsgeber (10) vorhandenen Speicherelement(en) (12, 12') insgesamt zwei oder mehrere verschiedene Verschlüsselungsalgorithmen (A1, A2, ...) abgelegt sind, die von dem/den Mikroprozessor(en) (11, 11') wahlweise in Zuordnung zu dem jeweils angesprochenen Objektmodul (1, 2) aufrufbar sind.

2. Zugangsberechtigungskontrolleinrichtung nach Anspruch 1, dadurch gekennzeichnet, daß die Zuordnung des zu verwendenden Verschlüsselungsalgorithmus (A1, A2, ...) zu dem jeweiligen Objektmodul (1, 2) durch einen einmaligen Initialisierungsvorgang festgelegt ist.

3. Schlüssellose Zugangsberechtigungskontrolleinrichtung mit zumindest zwei, jeweils einem bestimmten Objekt zugeordneten, Sende-/Empfangseinrichtungen umfassenden Objektmodulen (1, 2) und mit einem oder mehreren Identifikationsgebern (10), wobei jeweils über eine bidirektionale Datenkommunikationsstrecke (14, 15) Daten zwischen

dem Identifikationsgeber (10) und den Objektmodulen (1, 2) übertragbar sind, welche Daten mittels eines einen Verschlüsselungsalgorithmus sowie dem jeweiligen Objektmodul (1, 2) zugeordnete Verschlüsselungsparameter (P1, P2) verwendenden, symmetrischen Verschlüsselungsverfahrens codiert sind, **dadurch gekennzeichnet,** daß in einem in zumindest einem Objektmodul (1, 2) vorhandenen Speicherelement (8, 9) zwei oder mehrere verschiedene Verschlüsselungsalgorithmen (A1, A2, ...) abgelegt sind, wobei der jeweils zu verwendende Verschlüsselungsalgorithmus in Zuordnung zu dem verwendeten Identifikationsgeber (10) festlegbar ist.

4. Zugangsberechtigungskontrolleinrichtung nach Anspruch 3, dadurch gekennzeichnet, daß die Zuordnung des zu verwendenden Verschlüsselungsalgorithmus zu dem jeweiligen Identifikationsgeber (10) durch einen einmaligen Initialisierungsvorgang festgelegt ist.

5. Identifikationsgeber für eine schlüssellose Zugangsberechtigungs-kontrolleinrichtung zum Austauschen von Daten mit Objekten zugeordneten, Sende-/Empfangseinrichtungen (4, 5) umfassenden Objektmodulen (1, 2), welche Daten in einem Mikroprozessor (11, 11') mittels eines einen Verschlüsselungsalgorithmus sowie dem jeweiligen Objektmodul (1, 2) zugeordnete Verschlüsselungsparameter (P1, P2) verwendenden, symmetrischen Verschlüsselungsverfahrens codiert sind, **dadurch gekennzeichnet,** daß in (einem) Speicherelement(en) (12, 12') insgesamt zwei oder mehrere verschiedene Verschlüsselungsalgorithmen (A1, A2, ...) abgelegt sind, die von dem/den Mikroprozessor(en) (11, 11') wahlweise in Zuordnung zu dem jeweils angesprochenen Objektmodul (1, 2) aufrufbar sind.

6. Identifikationsgeber nach Anspruch 5, dadurch gekennzeichnet, daß zumindest die in einem Speicherelement (12, 12') abgelegten Verschlüsselungsalgorithmen (A1, A2) über eine Programmierschnittstelle manipulierbar und/oder austauschbar sind.

7. Identifikationsgeber nach Anspruch 5 oder 6, dadurch gekennzeichnet, daß zumindest ein Speicherelement (12, 12') in einem zugeordneten Mikroprozessor (11, 11') integriert ist.

8. Objektmodul für eine schlüssellose Zugangsberechtigungskontrolleinrichtung mit einer Sende-/Empfangseinrichtung (4, 5) zum Austauschen von Daten mit einem Identifikationsgeber (10) , welche Daten mittels eines einen Verschlüsselungsalgorithmus sowie dem Objektmodul zugeordnete Verschlüsselungsparameter (P1, P2) verwendenden, symmetrischen Verschlüsselungsverfahrens codiert sind, **dadurch gekennzeichnet,** daß in einem Speicherelement (8, 9) zwei oder mehrere verschiedene Verschlüsselungsalgorithmen (A1, A2, ...) abgelegt sind, wobei der jeweils zu verwendende Verschlüsselungsalgorithmus in Zuordnung zu dem verwendeten Identifikationsgeber (10) festlegbar ist.

9. Objektmodul nach Anspruch 8, dadurch gekennzeichnet, daß die in dem Speicherelement (8, 9) abgelegten Verschlüsselungsalgorithmen (A1, A2, ...) über eine Programmierschnittstelle manipulierbar und/oder austauschbar sind.

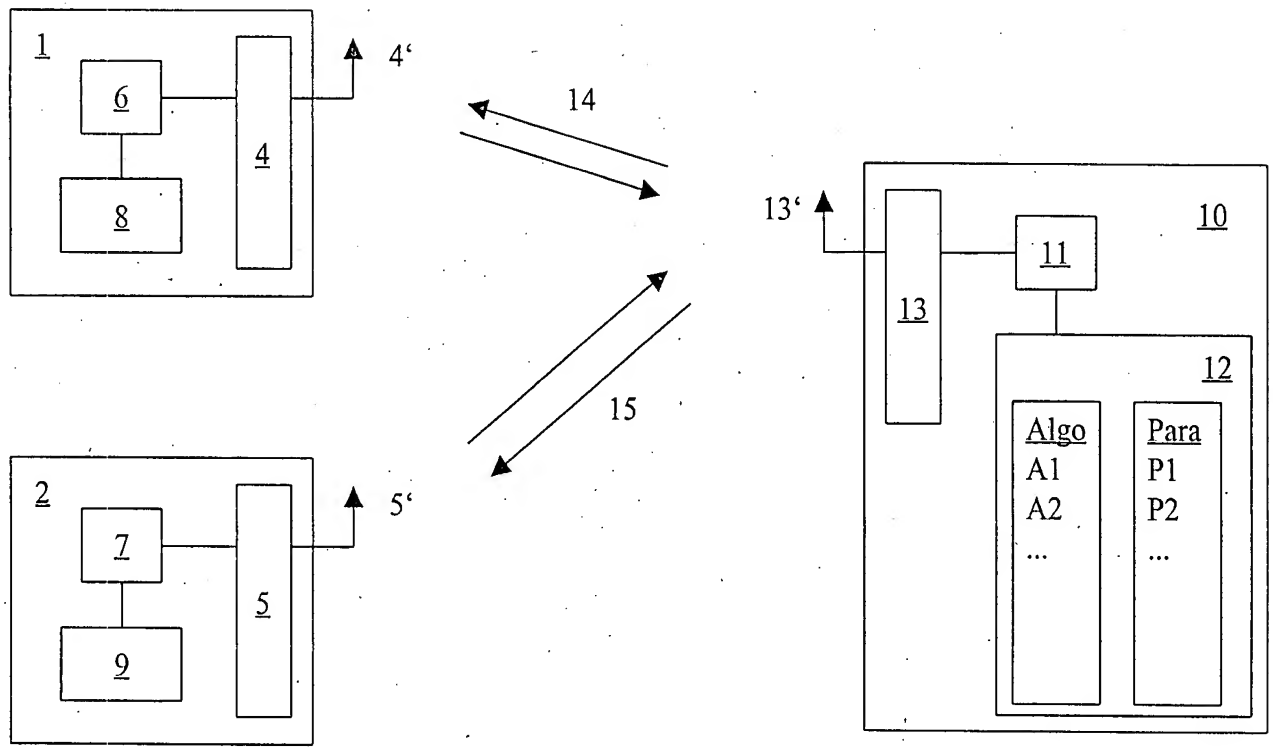

Fig. 1

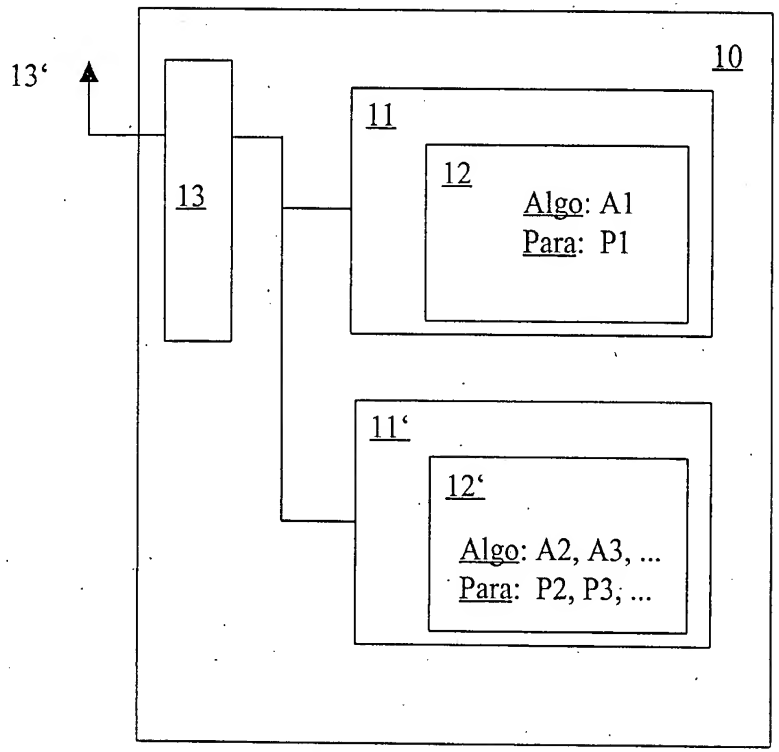

Fig. 2